Ordine degli Ingegneri di Firenze
Ordine Degli Ingegneri Della Provincia Di Firenze
Viale Milton 65 - 50129 Firenze -
19 settembre 2018 14:00–18:15

Bitcoin e criptovalute

Filosofia, economia e tecnologia della nascita di Bitcoin

Marco A. Calamari
marco.calamari@ordineingegneripisa.it

IISFA – International Information Systems Forensics Association: Italian Chapter

Il vostro anfitrione

https://www.linkedin.com/in/marcocalamari/

- **Marco Calamari, classe 1955, ingegnere nucleare, ha lavorato come architetto di applicazioni ed e' specializzato in gestione di programmi sorgenti legacy. Oggi si cimenta a rotazione in attivita' di consulenza informatica, Computer Forensics, editoriali e formazione.**
- **Affiliazioni: IISFA, ONIF, AIP, Opsi, Hermes Center, PWS**
- **Appassionato di privacy e crittografia, ha contribuito ai progetti FOSS Freenet, Mixmaster, Mixminion, Tor e Globaleaks.**
- **Fondatore del *Progetto Winston Smith* e del *Centro Hermes per la Trasparenza ed i diritti digitali*.**
- **Dal 2003 scrive su Punto Informatico ed altre riviste la rubrica "Cassandra Crossing", che ha superato le 400 uscite. (www.cassandracrossing.org)**

Il corso

Di Bitcoin si parla molto, ma di informazioni oggettive su di esso ne circolano poche; essendo un oggetto informatico con applicazioni economiche è necessario studiarlo da ambedue i punti di vista prima di poterlo valutare, ed a maggior ragione utilizzarlo in maniera razionale e priva di rischi.

Si parla infatti di Cryptoeconomics.

Il corso è finalizzato a fornire una panoramica generale della materia, per mettere in grado un professionista di orientarsi e poter valutare necessità, opportunità e possibilità di utilizzo di bitcoin.

Il corso è introduttivo, destinato a persone non specializzate nel settore; sono comunque utili, anche se non indispensabili, conoscenze elementari di informatica e/o di economia.

Di cosa parleremo

Prima parte

Denaro, denaro contante, denaro nella finanza, transazioni elettroniche, valute sintetiche, criptovalute.

Seconda parte

Breve storia della crittografia e delle criptovalute;
Elementi di crittografia

Terza parte

Tecnologie in Bitcoin: dalla crittografia ed i certificati alle blockchain.

Quarta Parte

Funzionamento di Bitcoin; conio, notariato e P2P.

Parte prima

Dal denaro contante alle criptovalute

Il panorama economico

Il fenomeno economico del terzo millennio non e' stata la crisi dei mutui subprime e neppure la bolla delle dot.com.

Il fenomeno economico del terzo millennio e' stato la nascita delle valute digitali come Bitcoin, Ethereum e la dozzina di valute minori che li hanno seguiti.

Il fatto che fa notizia e' la crescita vertiginosa del valore del Bitcoin negli ultimi due anni.

Tuttavia la vera notizia e' che esistano persone, aziende ed istituzioni che considerano una sequenza di bit equivalente ad una valuta nazionale, e che siano cosi' tante da portare il circolante totale delle criptovalute alla dimensione delle centinaia di miliardi di dollari.

I beni di scambio

Il primo sistema di scambio di beni e servizi e′ stato il baratto. Molto semplice da gestire, diventa complesso quanto il numero di possibili beni da scambiare e′ elevato. E′ difficile che ambedue le parti di una transazione possano avere direttamente quello di cui hanno bisogno. Spesso diventano necessari passaggi intermedi.

Un bene di scambio risolve il problema. Si tratta di qualcosa con un valore d′uso intrinseco che tutti condividono, e che puo′ essere utilizzato nelle transazioni in cambio od in pagamento di un bene.

Il sale in panetti e′ stato anticamente usato in Cina per questo scopo. Il termine *salario* deriva infatti dall′uso romano di pagare i soldati con sale.

Anche oro ed argento sono stati beni di scambio.

La moneta

Il controllo di uno stato od organizzazione sociale sul mezzo di scambio e' importante quanto lo e' quello sull'economia e sulle tasse.

Per questo motivo gli stati hanno trasformato nella storia i beni di scambio in moneta, applicando su di essi un riconoscimento ufficiale.

Nel caso piu' antico, quello del sale, il governo cinese dell'epoca applicava un sigillo a fuoco sui panetti di sale.

Questo tipo di moneta era fisicamente fragile; umido e cadute la distruggevano. Per risolvere il problema era possibile convertire 10 monete danneggiate in 9 nuove, sottolineando il fatto che il sale ufficiale "valeva" piu' di quello ordinario.

Si trattava quindi non piu' di un bene di scambio ma di una moneta, dotata pero' di valore intrinseco.

Il denaro

Come gia’ accennato, la maggior parte delle economie ha utilizzato metalli preziosi, a partire dal rame fino ad oro ed argento, per coniare monete pratiche, durevoli e di facile riconoscimento.

Le monete antiche erano dotate di un valore intrinseco, anche se gia’ nella storia antica questo valore veniva, per quanto possible, abbassato da chi le coniava per aumentare la quantita’ di monete coniabili a parita di metallo prezioso disponibile.

Monete d’oro con anima di altro metallo e monete di metalli preziosi in lega con metalli di valore inferiore erano comuni.

In tempi moderni il valore della moneta e’ stato sganciato da quello intrinseco, garantendo la convertibilita’ aurea a tasso fisso, e permettendo l’emissione di banconote prive di valore intrinseco.

Il denaro moderno

A partire dal ‘900 le economie degli stati moderni, e non e’ questa la sede per entrare nei particolari, hanno iniziato a regolare la convertibilita’ in oro.

Il sistema aureo fu sostituito dagli accordi di Bretton Woods del 1944, che furono efficaci fino al 15 agosto 1971, quando gli USA abolirono la convertibilità del dollaro in oro, decretando di fatto la morte del sistema aureo e la nascita del sistema fluttuante.

In un sistema fluttuante il valore di una moneta, ormai ridotta ad un pezzo di carta o ad una scrittura contabile, e’ stabilito da interazioni dirette con l’economia dello stato che la emette.

Il denaro contante circolante e’ poi solo una piccola frazione del circolante totale, che consiste principalmente in scritture contabili.

Valute e tassi di cambio

Nelle moderne economie fluttuanti il valore del denaro e' spesso stabilito in relazione ad una valuta nazionale diversa, di solito usata come riferimento.

Sono le valute emesse dai paesi con economie piu' forti ad essere prese come riferimento.

Al giorno d'oggi sono il Dollaro (USD-$) e l'Euro (EUR-€), con lo Yen (JPY-¥) e lo Yuan (CNH-¥)che li stanno affiancando.

Il tasso di cambio di una valuta nazionale normale o debole con una forte diviene quindi una misura del valore relativo delle due valute nazionali.

Esiste un fenomeno che diminuisce il valore assoluto di una moneta rispetto ad un bene, che e' comunemente detto inflazione.

Abolizione del contante

La tendenza attuale e' quella di una progressiva abolizione del denaro contante in favore di scritture contabili in forma di transazioni elettroniche, anche nel caso di pagamenti ordinari di piccola entita'.

La Svezia e' il paese piu' avanzato in questo percorso, arrivando a rendere possibile ai pubblici esercizi il rifiuto del denaro contante, rifiuto dovunque e sempre vietato *ope legis*.

L'uso coatto di transazioni elettroniche apre enormi problemi di privacy e controllo sociale, che non e' possibile pero' affrontare in questa sede.

Tuttavia anche in un mondo senza contante la valuta corrente e' sempre la stessa, inalterata.

Le transazioni elettroniche non sono infatti denaro elettronico (o meglio denaro digitale).

Parte seconda

Breve storia della crittografia

Cenni storici...

La storia della crittografia copre quattro millenni, ma puo' essere riassunta con una manciata di nomi e di fatti.

circa 450 a.e.v. - Erodoto racconta la storia di un nobile persiano che fece rasare i capelli ad uno schiavo fidato, gli fece tatuare un messaggio sul cranio, attese fino a quando i capelli furono ricresciuti e lo invio' a destinazione con l'istruzione di rasarsi nuovamente i capelli una volta arrivato. Metodo con larghezza di banda limitata, forte latenza ed oltretutto e' steganografia, non crittografia.

58 a.e.v. - Gaio Giulio Cesare usa e piu' tardi descrive nel *"De Bello Gallico"* il *cifrario cesariano*, o di sostituzione monoalfabetica, per corrispondere con Lucio Cornelio Balbo Maggiore mentre era impegnato nelle sue campagne militari. Primo esempio moderno di separazione tra chiave ed algoritmo, usato oggi solo alle elementari per scambiarsi bigliettini che la maestra non dovrebbe riuscire a leggere..

Cenni storici...

1586 p.e.v. – nel *“Traité des Chiffres”* Blaise de Vigenère descrive il primo metodo storico di sostituzione polialfabetica; metodo sempre con chiave separata dall’algoritmo, ma infinitamente piu’ “robusto”. Questi algoritmi sono detti a chiave singola o chiave privata.

1941 p.e.v. – Konrad Zuse costruisce lo Z3 il primo elaboratore automatico non meccanico controllato da un programma.

1976 p.e.v.: l'NSA ed il governo americano eleggono un algoritmo crittografico a chiave privata, proposto in maniera non troppo indipendente da IBM, a standard crittografico FIPS federale (DES).

Cenni storici...

circa 1970 p.e.v. - varie persone hanno una idea rivoluzionaria, la crittografia a chiave pubblica. che permette di evitare lo scambio delle chiavi tra i corrispondenti.

Scoperta da James Ellis, impiegato dell'MI5 intorno al 1970, e chiusa in un cassetto dai suoi capi fino al 1997, prima perche' non ne avevano capito l'importanza e poi probabilmente per la vergogna o per non essere silurati.

Riscoperta in maniera sostanzialmente indipendente da Withfield Diffie e Martin Hellmann nel 1976 (DH), e da Ron Rivest, Adi Shamir e Leonard Adleman al MIT nel 1977 (RSA). Diffie vi sarebbe stato simpatico, un vero personaggio. Anche per gli standard degli anni '70 era un fricchettone eccezionale, geniale e motivato alla Stallmann o meglio alla Wau Holland.

Cenni storici...

Nel 1981 David Chaum introdusse, teorizzo' e sistematizzo' il concetto di **Mix-net**, cioe' di rete paritaria di scambio di messaggi cifrati.

Nel 1986 una famosa querelle giuridica, scatenata da una causa promossa dalla **religione di Scientology,** provoca la reazione del gruppo **Cypherpunks** e la nascita dei sistemi crittografici di comunicazione moderni, implementando per la prima volta in maniera crittograficamente robusta il meccanismo delle **Mixnet**.

Nel 1991 **Philip R. Zimmermann**, un programmatore freelance di Boulder, Colorado, pubblica in Rete **PGP** - **Pretty Good Privacy**, il primo programma di crittografia forte disponibile al pubblico. Il nome e' preso da una sitcom radiofonica dell'epoca, in cui esisteva un emporio di frutta e verdura "Pretty Good Grocery". Il nome e' tuttavia inesatto, perche' la privacy garantita da PGP non e' *"piuttosto buona"* ma "eccezionale".

Cenni storici...

Negli anni '90 Paul Syverson ed altri definirono l'incapsulamento crittografico per il routing di pacchetti di informazioni, il cosiddetto Onion Routing .

Il concetto di Blockchain fu descritto per la prima volta nel 1991 da Stuart Haber e W. Scott Stornetta, e meglio definito nel 1996 da Ross J. Anderson e nel 1998 da Bruce Schneier and John Kelsey.

Nel 1998, Nick Szabo definiva un meccanismo per la creazione di una moneta digitale decentralizzata che battezzo' gold. Nel 2000 Stefan Konst pubblica una teoria generale per le blockchain ed una serie di regole pratiche per la loro implementazione

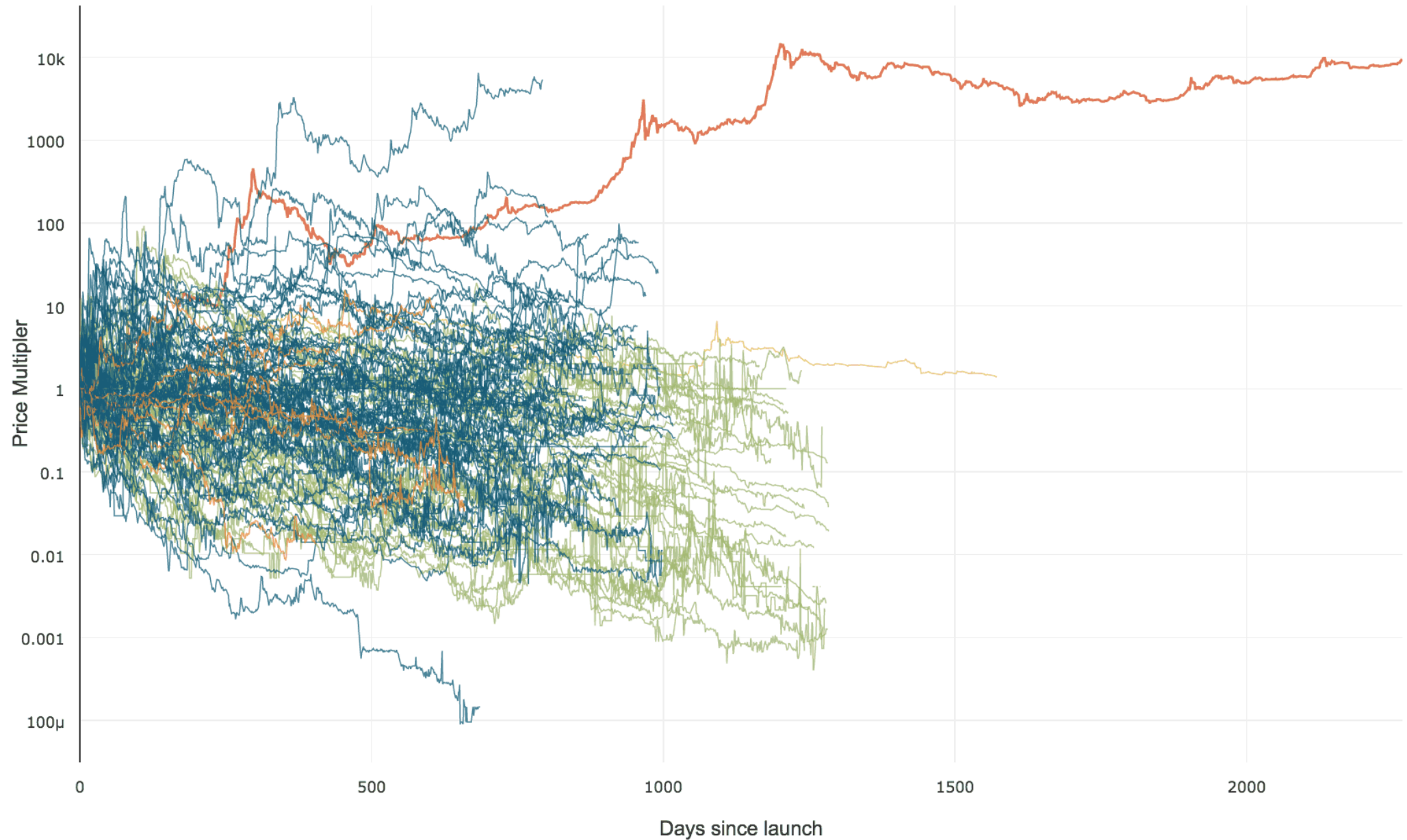
La prima blockchain distribuita fu implementata da Satoshi Nakamoto (persona che brilla per la sua inesistenza) nel 2008 e realizzata nel 2009 come parte fondamentale della moneta digitale Bitcoin, dove e' utilizzata come registro pubblico di notariato per le transazioni.

Ed oggi di quanti soldi parliamo?

Su Coinmarketcap.com alla data odierna sono elencate 1486 criptovalute.

Tra queste ce ne sono 34 con oltre un miliardo di dollari di circolante.

Il circolante di Bitcoin ฿ vale 200 miliardi di dollari, quello di Ethereum 100.

Valore delle criptovalute – giorni dal lancio

Definizioni

Funzione di hash

Una funzione di hash legge un file di lunghezza arbitraria e produce un'impronta digitale di lunghezza fissa.

Ad esempio, SHA-256 produce una impronta digitale di 64 caratteri esadecimali (equivalenti a 32 byte) come questa:

73098ab8b8a3233e9166e5aca0c40261

f08e55bc1585e9c6fa745e9d1cfad1fe

La proprieta' essenziale di una funzione di Hash e' che e' molto semplice calcolare l'impronta digitale di un file, ma che variando anche solo un carattere del file, l'impronta cambia completamente in maniera impredicibile.

E' inoltre computazionalmente impossibile trovare un file diverso che abbia la stessa impronta digitale.

Questo significa che se il file contiene un testamento in formato PDF, non e' in pratica possibile realizzarne una versione alterata che contenga un nome di erede diverso.

Algoritmi a chiave simmetrica

Esistono algoritmi matematici (detti crittografici) a chiave simmetrica, detti anche a chiave privata od a chiave singola in grado di cifrare un file e renderlo illeggibile, applicandovi una password di lunghezza predeterminata.

Per alcuni di questi algoritmi, utilizzando opportune lunghezze di password (chiave), la violazione della cifratura e′ dimostratamente impossibile anche con potenze di calcolo enormi.

Applicando con la stessa chiave una seconda volta l′algoritmo di cifratura, e′ possibile decifrare il file; da questa proprieta′ discende appunto la denominazione di algoritmo a chiave simmetrica.

Algoritmo a chiave asimmetrica

Esistono algoritmi crittografici che prevedono l'utilizzo di una coppia di chiavi, chiamate rispettivamente pubblica e privata. Tali algoritmi vengono chiamati anche a chiave doppia o a chiave pubblica.

Le due chiavi di una coppia possiedono una proprieta' di simmetria totale,; cio' che una cifra solo l'altra decifra. Non e' necessario lo scambio di chiavi, poiche' la chiave pubblica di tutte le coppie, che permette solo di cifrare e non di decifrare, puo' essere diffusa e condivisa liberamente.

Non e' quindi necessario conoscere ed aver interagito col destinatario per inviare un messaggio cifrato; basta reperire la sua chiave pubblica su uno degli appositi server, ed essere sicuri che essa appartenga al destinatario.

Firma digitale

Ricodiamo che le due chiavi di una coppia di chiavi asimmetriche possiedono una proprieta' di simmetria; quello che una cifra solo l'altra decifra.

Calcolando l'hash di un file e criptando l'impronta con una chiave privata, si ottiene una firma digitale del documento originale.

Chiunque puo' prendere la chiave pubblica del firmatario, decodificare l'hash e verificare che e' proprio quello del documento.

Il firmatario quindi garantisce l'originalita' del documento, esattamente come una firma autografa.

Nella firma digitale a norma di legge italiana (eIDAS, EU 910/2014), le chiavi ed i certificati sono generati e memorizzati in una smartcard od in un dispositivo di firma.

Certificati digitali

Un certificato digitale e' un tipo particolare di firma digitale. Infatti e' la firma digitale di una chiave pubblica, completata con ulteriori informazioni.

Il firmatario di una chiave pubblica viene normalmente indicato come Autorita' di Certificazione o Certificatore.

Possono esistere piu' livelli di Certificatori, in cui il certificatore di livello superiore garantisce la chiave pubblica di quello di livello inferiore

Un Certificatore garantisce che la chiave pubblica per la quale ha emesso il certificato appartiene effettivamente ad una data persona, e che le eventuali informazioni aggiuntive allegate sono corrette.

Esempi di informazioni aggiuntive sono: nome, cognome, codice fiscale, data e luogo di nascita, residenza, posta elettronica, data di emissione, data di scadenza e per cosa il certificato puo' essere usato.

Marcatura temporale

Una marca temporale e' un tipo particolare di certificato digitale. La marca temporale certifica la data di firma di un documento. Il meccanismo di marcatura temporale funziona solo online:

1) l'applicazione richiede una marca temporale;

2) il certificatore temporale "batte" una marca contenente la data e la trasmette al richiedente;

3) l'applicazione inserisce nella marca l'hash del documento, firma la marca, produce un nuovo documento (.m7m) che contiene anche una copia della marca, e trasmette la marca al certificatore;

4) il certificatore, se la marca e' stata ritornata entro un certo intervallo di tempo stabilito, la archivia come valida. La marca archiviata comprende l'hash del documento ma non il suo contenuto.

Valuta digitale

Una valuta digitale e' una moneta sintetica definita solo in termini di informazione (bit).

Dovendo obbligatoriamente impiegare tecniche crittografiche e' anche detta criptovaluta.

Non e' correlata a nessuna moneta fisica o bene di scambio, e non e' attualmente adottata da nessuno stato nazionale.

E' stato oggetto di ricerca in campo matematico ed informativo, e definita nella sua accezione attuale da David Chaum nel 1982 nella fondamentale paper "*Blind signatures for untraceable payments*".

Ha avuto diversi tentativi di implementazione, iniziando dal 1983 con Digicash, ideato appunto di David Chaum, fino ad arrivare all'implementazione della prima valuta digitale entrata nell'uso reale, Bitcoin (XBT/BTC - ฿).

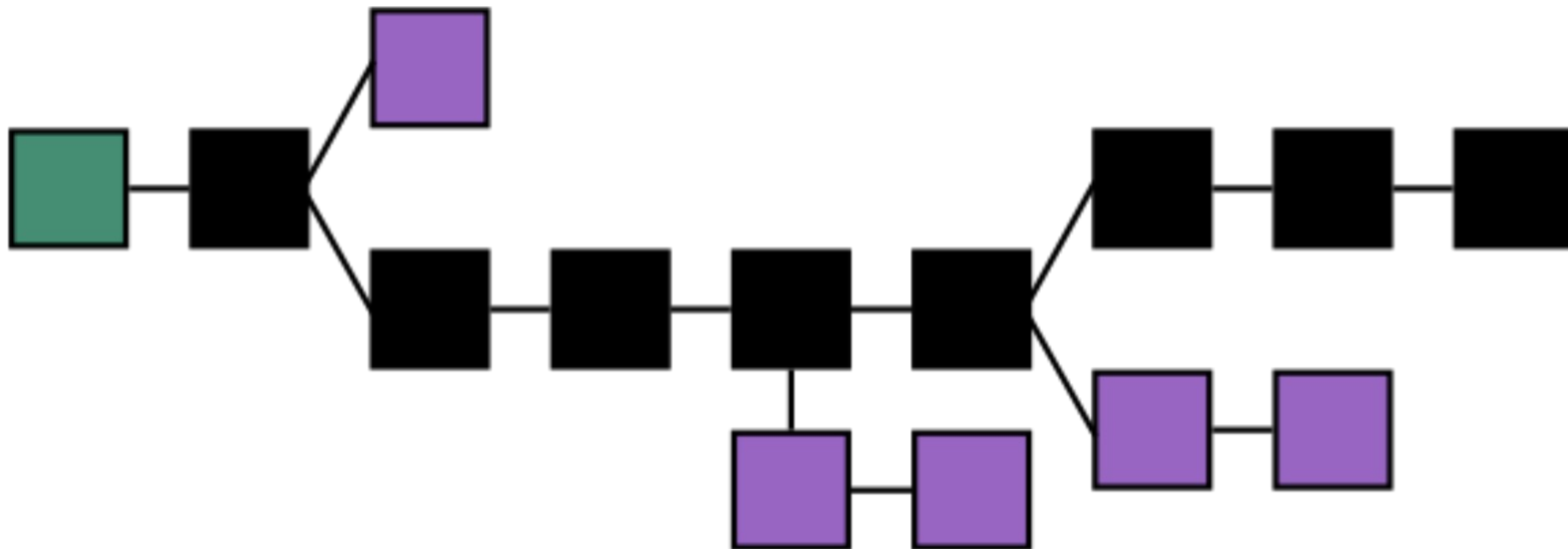
Parte terza

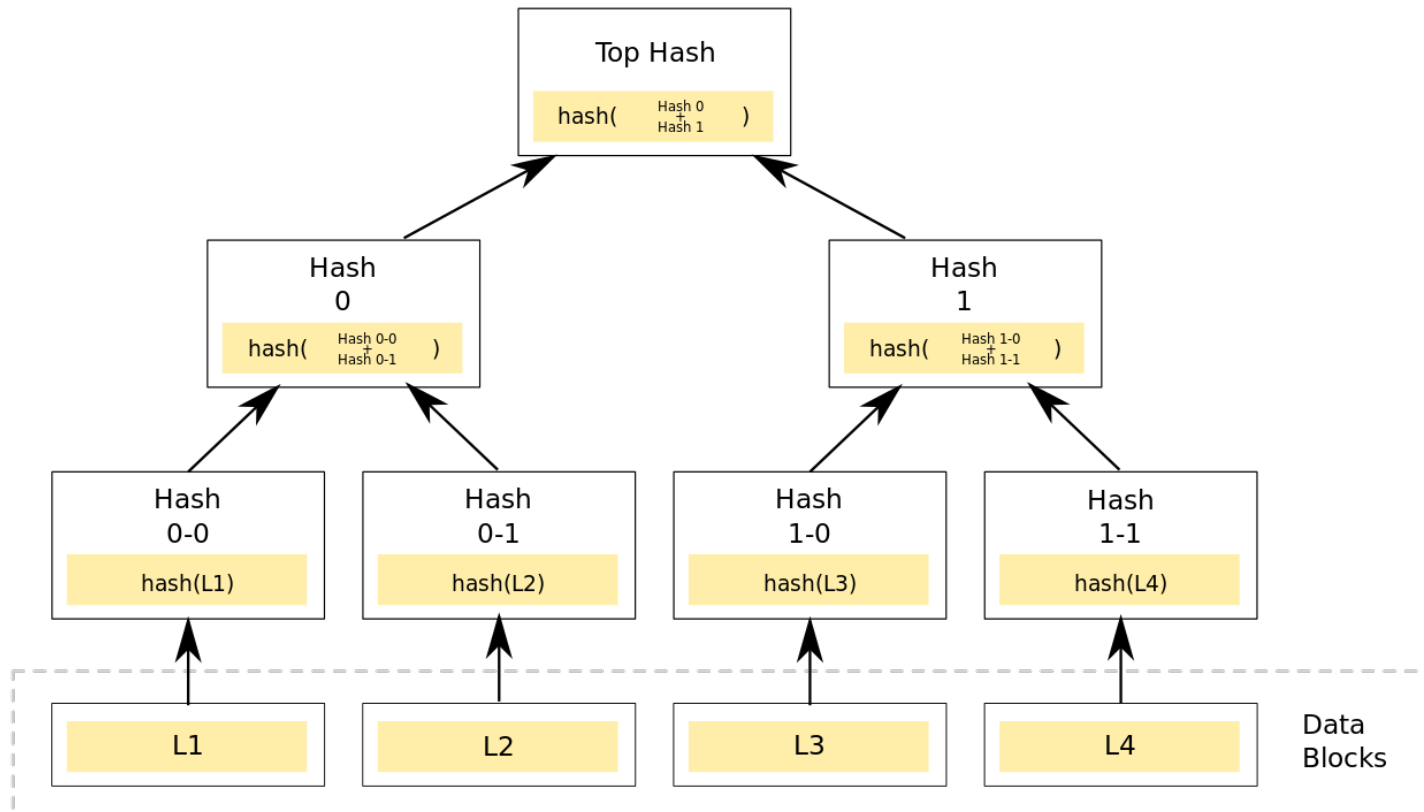
Tecnologie di Bitcoin

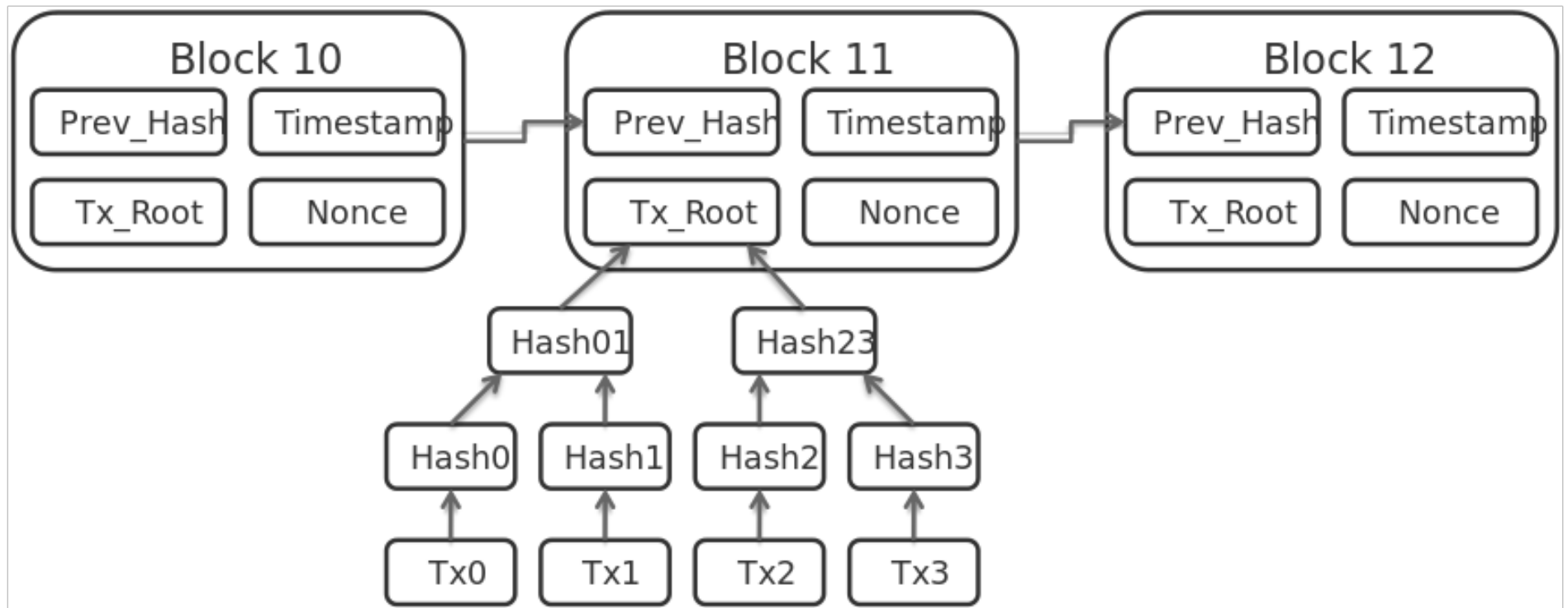
Blockchain

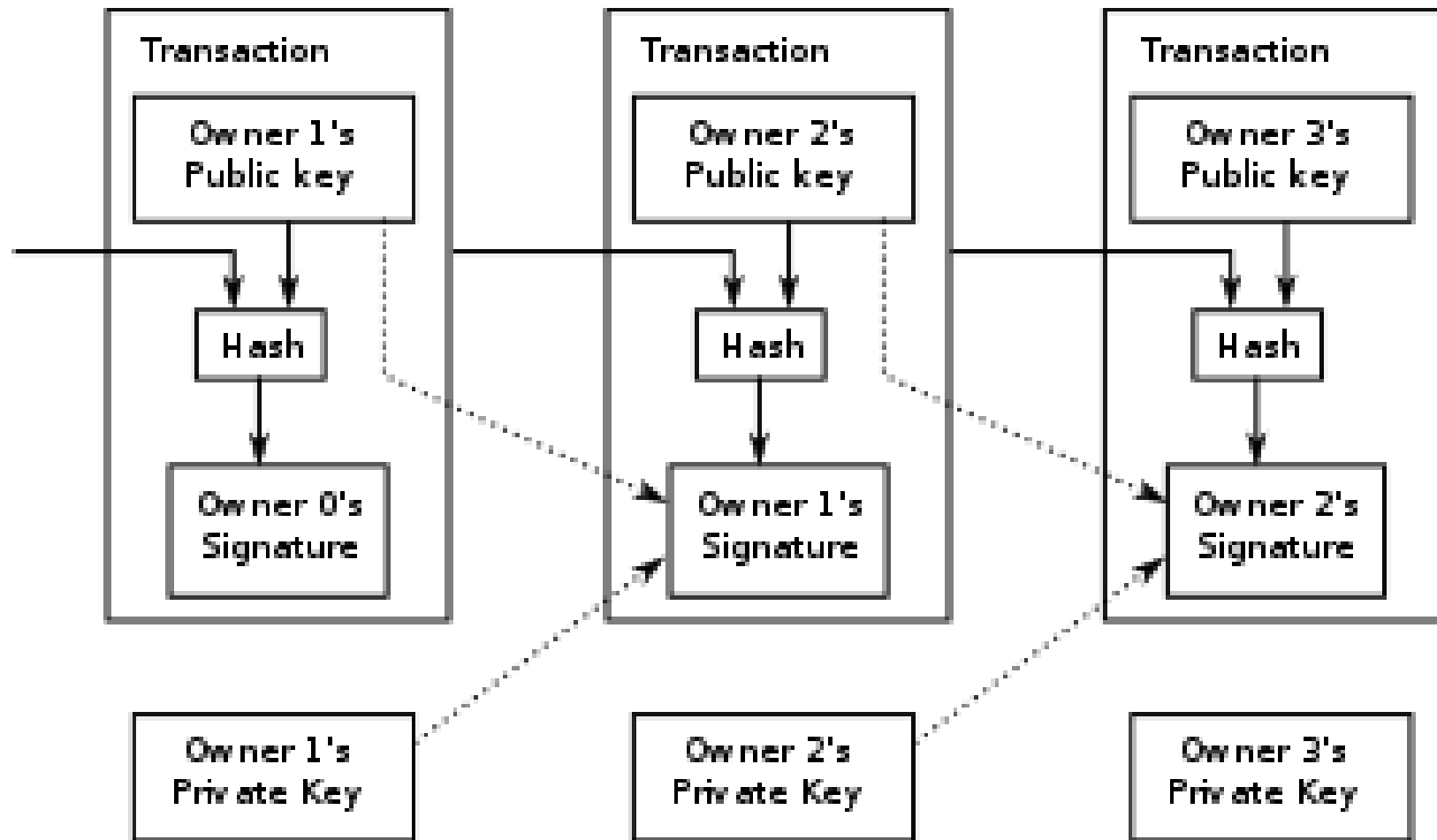
Una **blockchain** e' una struttura dati che permette di realizzare registri digitali di notariato in maniera semplice ed efficente.

Una blockchain e' costituita da una sequenza ordinata di blocchi di lunghezza variabile; ogni blocco contiene le informazioni di gestione ed una sequenza di oggetti (o file, senza perdere in generalita') di lunghezza e numero arbitrari.

La blockchain di Bitcoin e' **public** e **permissionless**.

Merkle tree

Come gia' accennato, il primo lavoro sulle blockchain fu pubblicato nel 1991 da Stuart Haber e W. Scott Stornetta. Nel 1992, Bayer, Haber e Stornetta incorporarono i Merkle tree alla blockchain per diminuire il numero di verifiche necessarie per poter convalidare un documento, e poter raccogliere più documenti in un unico blocco.

Struttura del blocco blockchain di Bitcoin

Ogni blocco della blockchain contiene, tra le informazioni di gestione, un hash crittografico del blocco precedente. Un blocco contiene una sequenza di transazioni i cui hash sono organizzati in un Merkle tree.

Struttura delle transazioni

Nel blocco della blockchain le transazioni della serie sono così strutturate:

Funzionamento di una transazione

Una transazione e′ dotata di uno o piu′ input ed uno o piu′ output.

Gli input provengono dagli output di transazioni precedenti che non sono stati ancora "spesi", e che vengono spesi nella nuova transazione.

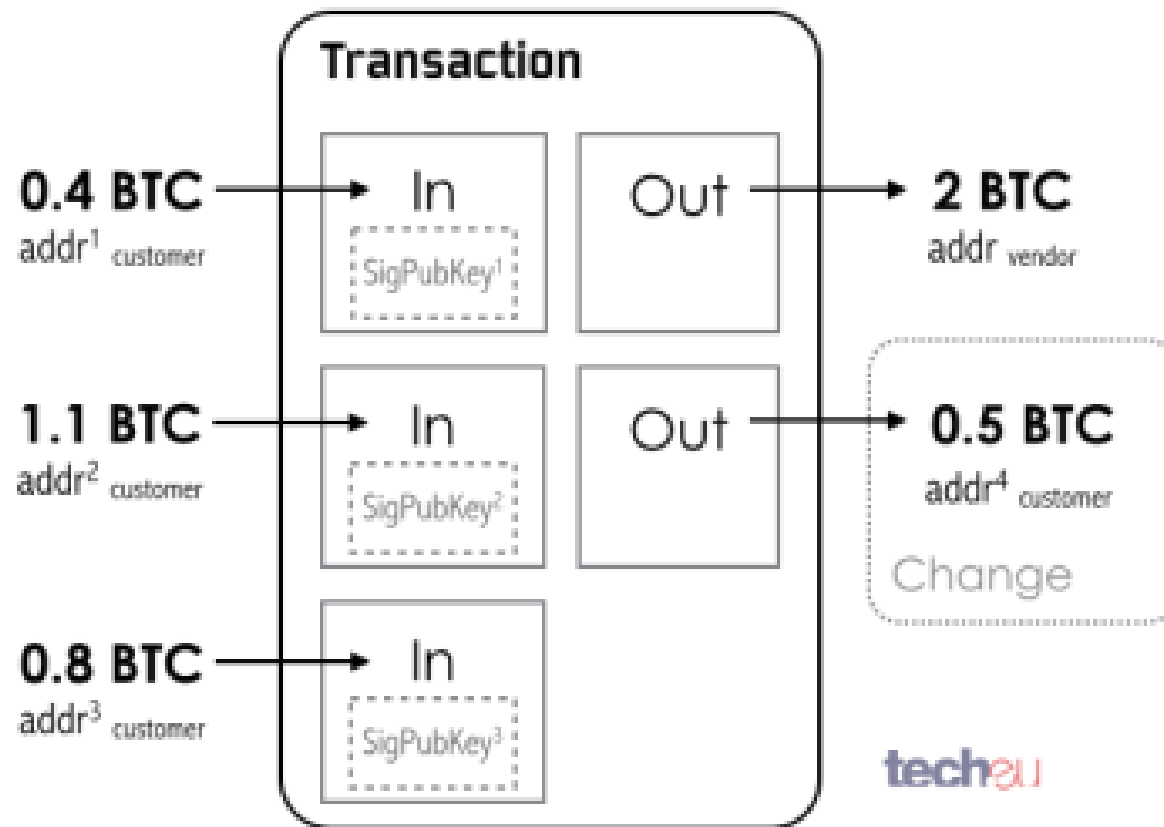
Gli output della nuova transazione sono ovviamente definiti come "non ancora spesi".

La somma di tutti gli output non spesi presenti in ogni momento nell′intera blockchain costituisce il circolante della rete/valuta Bitcoin.

Si, e′ proprio vero e ricordatelo sempre; i Bitcoin non esistono. Esistono solo le transazioni.

Funzionamento di una transazione

Ogni singola transazione contiene le proprie informazioni di gestione, gli input ed output della transazione, la chiave pubblica del proprietario, la firma del proprietario sulla transazione.

Facciamo l'esempio di una transazione per inviare 2 BTC ad un venditore in pagamento di una merce.

Registro di notariato

Ogni nuovo blocco certifica l'integrita' del blocco precedente, e per iterazione l'integrita' della intera blockchain.

L'entita' che firma digitalmente un nuovo blocco della blockchain certifica quindi non solo il blocco stesso ed i file in esso contenuti, ma l'integrita' dell'intera blockchain.

La blockchain permette di realizzare direttamente un registro di notariato; con questo si possono costruire applicazioni snelle e sofisticate, complesse od impossibili se realizzate con un normale database.

Nota: un vero notary service e' definito formalmente da ISO 13888, come il registro che fornisce i cripto asset per eseguire un protocollo di non ripudiabilita' per identificare i partecipanti.

Proof of work

Riporta Wikipedia: Un sistema proof-of-work (PoW) o protocollo proof-of-work, o funzione proof-of-work è una misura tecnologica cntro attacchi di denial of service (DoS - diniego di servizio) ed altri abusi come lo spam, imponendo un "costo" al richiedente del servizio per ricevere il servizio stesso; di solito il costo consiste in tempo di elaborazione.

La caratteristica chiave di un PoW e' l'asimmetria: il lavoro deve essere oneroso (ma fattibile) dal lato richiedente, e facile da verificare per il fornitore del servizio.

Bitcoin richiede come proof-of-work a chi certifica un nuovo blocco di prendere l'hash del blocco (che è un numero) e concatenarlo con un altro numero a piacere in modo che l'hash della concatenazione sia minore di una "difficoltà" data (cioe' che l'hash calcolato inizi con un certo numero di zeri).

Parte quarta

Funzionamento di Bitcoin

₿itcoin: software

Come gia' ricordato, Bitcoin e' una moneta digitale, utilizzata come valuta sintetica, realizzata a fine 2008 dalla personalita' fittizia ed anonima di Satoshi Nakamoto, che l'ha implementata come software a sorgente aperto e libero.

Il software originale e tuttora utilizzato si chiama Bitcoin Core, e si trova oggi su Sourceforge; e' rilasciato sotto licenza MIT.

Bitcoin Core comprende sia la parte server, che definisce i nodi (server) della rete Bitcoin, che la parte client, che consente all'utente di gestire il proprio portafoglio (wallet) di Bitcoin.

Esistono numerosi software che implementano la sola parte client del protocollo Bitcoin, detti wallet manager, di piu' facile installazione ed utilizzo.

₿itcoin: caratteristiche

Bitcoin e'implementato utilizzando una blockchain distribuita e replicata in un sistema di nodi P2P zero-trust, cooperanti e paritetici.

Nel sistema P2P la partecipazione, la cooperazione e l'onesta' dei nodi e' incentivata economicamente.

I nodi non client detengono una copia completa ed in continuo aggiornamento della blockchain.

I nodi raccolgono a piacere alcune nuove transazioni non ancora notariate, le assemblano in un blocco, e tentano di eseguire la certificazione.

Il primo nodo che vi riesce, viene ricompensato con un numero di Bitcoin fissato dal sistema, attualmente pari a 12.5 Bitcoin, piu' tutte le commissioni associate alle transazioni notariate.

₿itcoin: wallet e chiave privata

Il numero totale di Bitcoin che sono stati o potranno essere minati e’ limitato, pari a 20,999,839.77085749, circa 21 milioni.

L’ultimo blocco della blockchain che generera’ una ricompensa sara’ il n.6.929.999, la cui creazione e’ prevista circa nel 2140.

Ricordate; i Bitcoin non esistono, esistono solo le transazioni.

Quindi non ci sono informazioni nel vostro wallet che non siano gia’ presenti e ricaricabili dalla rete Bitcoin ...

... a parte (sempre piu’ ovviamente) la chiave privata del vostro wallet ...

₿itcoin: l'importanza di sicurezza e backup

Gia', la chiave privata del vostro wallet...

...dove sta e quanto e' sicura?

La chiave privata del wallet e' cio che fa si che i Bicoin vostri siano vostri, e che possano essere utilizzati.

Se viene rubata, i Bitcoin diventano del nuovo, anche se solo temporaneo, possessore, che in pochi secondi puo' mandarli dove vuole.

Se viene persa i bitcoin sono persi, per sempre e per tutti. La crittografia forte funziona davvero!

Si stima che non meno del 20% dei Bitcoin minati siano stati persi; sono li, nella blockchain, valgono 40 miliardi, dicasi QUARANTA MILIARDI di dollari, e nessuno li potra' mai avere.

₿itcoin: wallet manager

Un wallet manager permette di gestire uno o piu' wallet in maniera semplice.

Un wallet, di solito un singolo file di dati del wallet manager, contiene una chiave privata che identifica il wallet, e una serie di indirizzi Bitcoin, che sono ulteriori coppie di chiavi.

I wallet di solito permettono di generare una frase di recupero del wallet. Sono 12 parole inglesi che vi consentiranno di rigenerare tutto il wallet e le sue chiavi anche nel caso di perdita catastrofica del file del wallet manager.

Se vi sembra strano che un wallet, i relativi indirizzi, la storia delle transazioni ed il saldo dei Bitcoin possa essere cosi' rigenerato, ricordate che i Bitcoin non esistono, e che le transazioni sono tutte interamente memorizzate nella blockchain.

Ƀitcoin: pagamenti

Per inviare Bitcoin ad un indirizzo e′ necessario (ovviamente) conoscere l′indirizzo stesso.

E′ (altrettanto ovviamente) necessario disporre nel proprio wallet di una somma adeguata al pagamento della somma da spedire piu′ le spese di transazione.

E′ opportuno lasciar calcolare le spese di transazione al wallet manager stesso.

Normalmente le spese di transazione sono proporzionali alla dimensione in kB della transazione stessa, che dipende dal numero di input ed output della transazione.

L′entita′ delle spese e′ inversamente proporzionale al tempo che sara′ necessario perche′ la transazione compaia nel sistema e sia poi confermata.

₿itcoin: pagamenti

Attualmente, nel caso normale di una transazione con 3 input+output, e con il cambio a 10.000 Euro, le spese sono di 7 euro per un tempo di 10 minuti per l'apparizione e 60 per conferma della transazione.

Una transazione e' in realta' confermata appena inserita nel successivo blocco della blockchain che viene certificato. La transazione si considera pero' ancora non congelata fino a quando non sono stati certificati i successivi 6 blocchi.

E' quindi fortemente consigliato attendere almeno il tempo necessario alla certificazione di 6 blocchi.

Esistono organizzazioni dette Mining Farm, che controllano anche il 20% della rete Bitcoin, la cui potenza di calcolo potrebbe permettere di calcolare fino a 6 blocchi "falsificati" ed appenderli alla blockchain, producendone una biforcazione e permettendo double spending ed altre infamita'.

₿itcoin: uso del wallet: transazioni

Ƀitcoin: uso del wallet: transazioni

Ƀitcoin: uso del wallet: transazioni

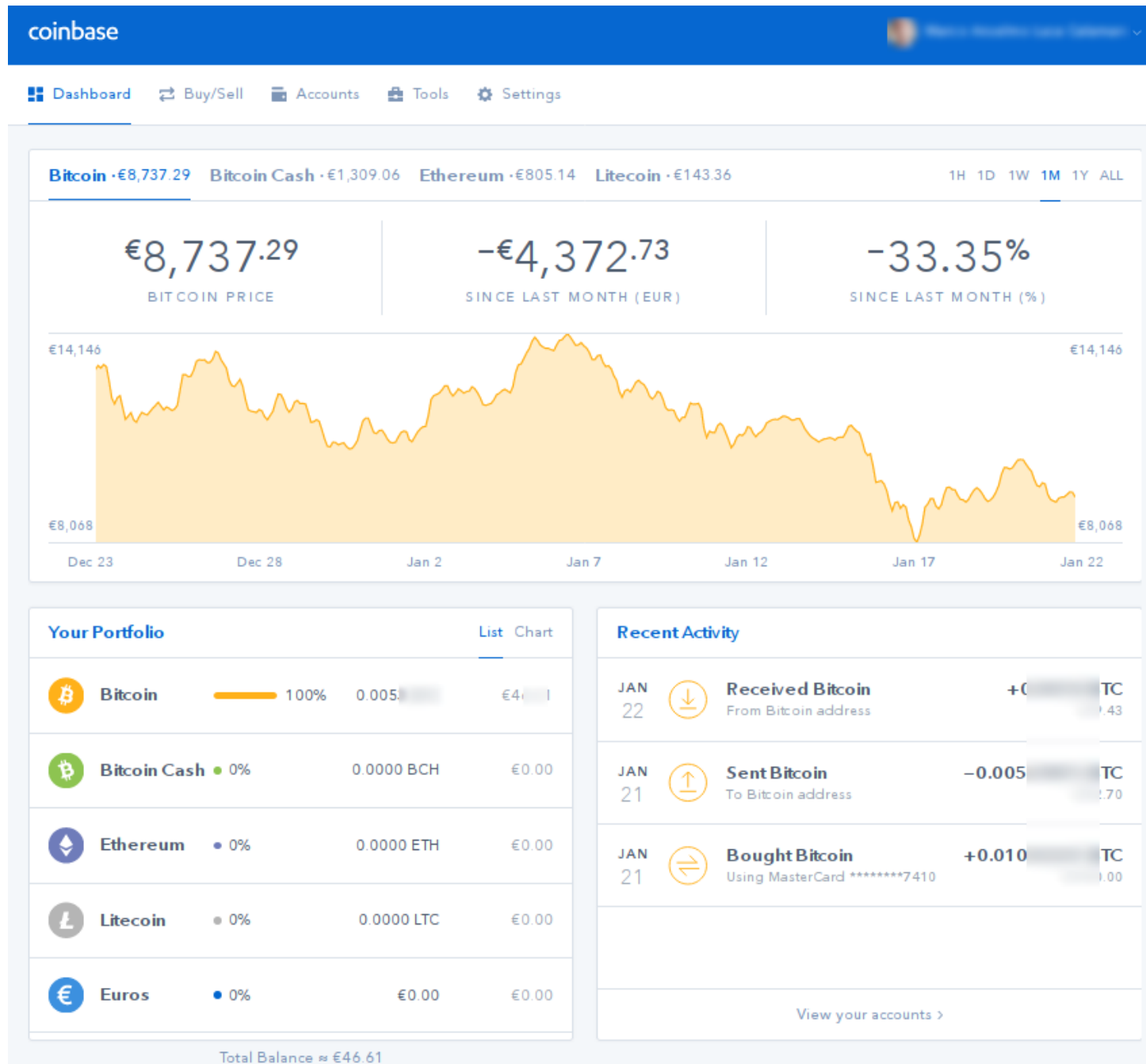
Electrum 2.7.9 - default_wallet [standard]

File Wallet Tools Help

History | Send | Receive | Addresses | Contacts | Console

Address	Label	Balance	Tx
▾ Receiving			
▾ Used			
1JI…KgDo		0.	2
1Jy9…EC		0.	0
1AnX…Jt4		0.	0
1Mna…zo		0.	0
1QAK…DH		0.	0
186U…HT		0.	0
▾ Change			
▸ 19yKI…c		3.3	1
1Dgd…yk		0.	0
1817…RE		0.	0
1DeW…Zp		0.	0
12Ua…mW		0.	0
1FsF…LM		0.	0
18yG…WQ		0.	0

Balance: 3.3 mBTC (No FX rate available)

Bitcoin: uso di wallet web e siti di exchange

Coniare Bitcoin

Coniare (minare) Bitcoin richiede una semplice installazione software e tanta, tanta, ma davvero tanta (ho detto “tanta”?) potenza di calcolo.

Mentre nel 2009 per minare poteva bastare un pc, oggi e’ necessario hardware ASIC dedicato, ed il consumo di energia elettrica rende comunque il minare antieconomico, almeno in occidente.

Coniare Bitcoin

Ogni transazione basata su Bitcoin (circa 300.000 al giorno) assorbe mediamente 215 kWh con picchi minimi che non scendono al di sotto dei 77 KWh. Parliamo quindi di circa 64 milioni di kWh al giorno, che richiede una potenza di 2700 MW, cioe′ di due grossi reattori nucleari moderni.

Considerando che viene minato un blocco ogni 10 minuti, cioe′ 240 al giorno parliamo di consumare circa 250 mila kWh per blocco, attivita′ che rende 12.5 bitcoin, pari a circa 20.000 kWh/BTC.

Con un costo (minimo) di 0.20 euro/kWh parliamo di spendere 4.000€ per ricavare 10.000€ (a cui aggiungere oneri finanziari e costi di struttura).

Conviene solo in Cina, dove hanno energia idroelettrica e da carbone da buttare. E la tendenza e′ senz′altro destinata a peggiorare.

Coniare Bitcoin

Ecco un capannone in Ordos, Mongolia interna, Cina, gia' citta' mineraria, poi ghost town ed oggi ...

Altre criptovalute

Attualmente esistono una trentina di criptovalute, significative, ma l'unico concorrente di Bitcoin, come circolante ma soprattutto come potenzialita' tecniche e'il sistema Ethereum.

Le criptovalute alternative a Bitcoin ed Ethereum presentano rischi speculativi decisamente superiori.

Alcune criptovalute possono essere scambiate solo via trading, e non direttamente.

Coinbase permette di fare trading su 5 di esse, ma solo alcune possono essere scambiate direttamente.

Siti come Trade.com permettono di cambiare e fare trading ma non scambiare direttamente criptovalute.

Coinmama e' un sito per il cambio di criptovalute.

Sia per il trading che il cambio valgono le normali raccomandazioni: occhio ai tassi e alle commissioni.

Il futuro, oggi: Ethereum

Riporta Wikipedia: *"Ethereum è una piattaforma decentralizzata … per la creazione e pubblicazione peer-to-peer di contratti intelligenti (smart contracts) creati in un linguaggio di programmazione Turing-completo)"*.

La moneta del sistema Ethereum, detta Ether (ETH-Ξ) consente di creare contratti intelligenti: e' quindi un denaro digitale altamente programmabile.

Per poter essere eseguiti sulla rete peer-to-peer, i contratti di Ethereum "pagano" l'utilizzo della sua potenza computazionale tramite l'unità di conto Ether, che funge quindi sia da criptovaluta che da carburante. Ethereum quindi non è solo un network per lo scambio di valore monetario ma un sistema per eseguire smart contract espressi in Ether. Questi contratti possono essere utilizzati in molti campi: sistemi elettorali, registrazione di nomi dominio, mercati finanziari, piattaforme di crowdfunding, proprietà intellettuale...

Grazie per l'attenzione

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+

PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698
DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B
Tel: (+39) 050 576031 Cell: (+39) 347 8530279
Fax: (+39) 050 7849817 Skype-Twitter: calamarim

+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ---------------+

Link utili - 1

Bitcoin su Wikipedia
https://it.wikipedia.org/wiki/Bitcoin

Chi e' Satoshi Nakamoto
https://it.wikipedia.org/wiki/Satoshi_Nakamoto

Calcolatore delle spese di transazione (inglese)
https://bitcoinfees.info/

Elenco dei siti di trading e cambio, e loro caratteristiche principali (inglese)
https://www.interactivecrypto.com/compare-all-bitcoin-exchanges-reviews/

Coinbase – sito di trading e cambio
https://www.coinbase.com/

Visualizzatore della blockchain di Bitcoin (inglese)
https://blockchain.info/

Calcolatore del costo per il mining di bitcoin (inglese)
http://www.alcula.com/calculators/finance/bitcoin-mining/

Elenco criptovalute e loro quotazioni (inglese)
https://coinfinder.it/

Articolo: una lettera per chi sta tentando di capire le criptovalute (inglese)
https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80

Link utili - 2

Articolo: cosa e’ la criptoeconomia (inglese)
https://blockgeeks.com/guides/what-is-cryptoeconomics/

Bitcoin Wiki: FAQ ufficiale su Bitcoin (inglese)
https://en.bitcoin.it/wiki/Help:FAQ

Forum su qualsiasi argomento correlato ai Bitcoin (inglese)
https://bitcointalk.org/

Browser della rete Bitcoin – dai grafici globali alle caratteristiche di ogni singola transazione
https://blockchain.info/it/charts

Hardware dedicato e costi per minare Bitcoin
http://www.portafoglioelettronicomigliore.com/bitcoin-asic-miner.asp

Consumo energetico real-time della rete Bitcoin
https://digiconomist.net/bitcoin-energy-consumption

In Cina, e piu’ precisamente in Mongolia, c’e’ Ordos, la zecca dei Bitcoin (inglese)
https://qz.com/1054805/what-its-like-working-at-a-sprawling-bitcoin-mine-in-inner-mongolia/

Come sono stati chiusi i siti del Dark Web deanonimizzando i Bitcoin
https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/

Elenco di Altcoin, i concorrenti di Bitcoin: Ether, Monero e le altre
https://www.bankrate.com/investing/12-cryptocurrency-alternatives-to-bitcoin/

Q&A time

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+

PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698
DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B
Tel: (+39) 050 576031 Cell: (+39) 347 8530279
Fax: (+39) 050 7849817 Skype-Twitter: calamarim

+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ---------------+